PERFORMANCE WORK STATEMENT (PWS)

Contractor Service Support of the Coalition and Allied Program's Collaboration at Sea (CAS) and Secure Releasable (SREL) Combined Enterprise Regional Information Exchange System-Maritime (CENTRIXS-M) Communications Systems

Navy Information Dominance Forces (NIDF)

March 26, 2015

List of Governing References

a. DoDD 8500.1, Information Assurance, 24 October 2002
b. DoDI 8500.2, Information Assurance (IA) Implementation, 6 February 2003
c. DoDI 8570.1M, Information Assurance (IA) Workforce Improvement Program, 24 January 2012
d. SECNAVINST 1543.2, CYBERSPACE/Information Technology Workforce Continuous Learning, 30 November 2012
e. DOD 5200.1-R, Information Security Program, January 1997
f. DoDD 5200.40, DOD Information Technology Security Certification and Accreditation Process (DITSCAP), 30 December 1997
g. DOD Directive 5205.8, Access to Classified Cryptographic Information, 20 February 1991
h. CJCSI 6211.02B, Defense Information System Network Policy, h. Responsibilities and Processes of 31 July 2003
i. CJCSM 6510.01, Defense-In-Depth: Information Assurance and Computer Network Defense of 25 March 2003 w/Ch-1
j. SECNAV 5239.3A, Department of the Navy Information Assurance Policy, 20 December 2004
k. Information Assurance Certification and Accreditation Process (DIACAP) Interim Guidance, 6 July 06
l. Navy Telecommunications Directive (NTD) 08-10 Navy Ports, Protocols, and Services (NPPS) for Navy Unclassified and Classified Networks
m. 5 USC 552a, The Privacy Act of 1974
n. Director of Central Intelligence 6-3, Security Policy on Intelligence Information in Automated Systems and Networks
o. NSTISSP No. 11 Revised, National Policy Governing the Acquisition of Information Assurance (IA) and IA Enabled Information Technology (IT) Products, June 2003
p. USN/USMC IA PUB-5239-22, Information Assurance Protected Distribution System (PDS) Publication, October 2003
q. DoD Directive 5000.1, Defense Acquisition System, November 2003
r. ISO 9000, Quality Management Systems, - Fundamentals and Vocabulary, April 2001
s. DOD Manual 5220.22-M, National Industrial Security Program Operating Manual (NISPOM)

SECTION 1 BACKGROUND AND GENERAL INFORMATION

1.1 GENERAL: This is a non-personal services contract to provide contractor personnel for the management, support, and operation of the Collaboration at Sea (CAS) and Combined Enterprise Regional Information Exchange System – Maritime (CENTRIXS-M) Coalition and Allied communications programs. CAS is a web based system used to convey mission essential information to a large group of users with low band-width consumption. CENTRIXS-M forms the network backbone and global infrastructure for coalition and multinational Command, Control, Communications, Computers, and Intelligence (C4I) interoperability. It provides secure tactical and operational information sharing between U.S. and coalition maritime partners.

1.2 TYPE OF CONTRACT: The Government intends to award an Indefinite Delivery/Indefinite Quantity contract with Firm-Fixed Price provisions for services and 'not to exceed' line items for other direct costs. Individual task orders will specify positions and performance locations.

1.3 OVERVIEW OF TASKS: Tasks consist of program and project management, network engineering support, information security, Information Assurance, Tier I, II, and III Service Desk Support, web applications programming and development, systems engineering, systems integration, software testing, configuration management, software deployment and version control, system technical documentation, user training, and operations support.

1.4 PERIOD OF PERFORMANCE: The period of performance shall be for a base year of twelve (12) months and four (4) 12-month option years. The Period of Performance reads as follows:

Base Year	11 September 2015 – 10 September 2016
Option Year I	11 September 2016 – 10 September 2017
Option Year II	11 September 2017 – 10 September 2018
Option Year III	11 September 2018 – 10 September 2019
Option Year IV	11 September 2019 – 10 September 2020

1.5 LOCATIONS OF PERFORMANCE: The work to be performed under this contract will be performed at US Government provided facilities in locations as specified in task orders issued under this contract. Contract performance may occur at any of the following sites.

a. USFLTFORCOM Headquarters facilities, Norfolk, VA
b. Navy Information Dominance Forces (NIDF), Suffolk, VA
c. United Atlantic Regional Network Operations Center (UARNOC), Norfolk, VA
d. Pacific Regional Network Operations Center (PRNOC), Honolulu, HI
e. International locations such as Netherlands, United Kingdom, Australia, Canada, Italy, Bahrain, New Zealand, Japan, and South Korea.
f. Other sites as dictated by the Government.

1.6 HOLIDAYS: The contractor is generally not required to provide services on these days.

New Year's Day	Labor Day
Martin Luther King Jr.'s Birthday	Columbus Day
President's Day	Veteran's Day
Memorial Day	Thanksgiving Day
Independence Day	Christmas Day

World events, system testing, and other emergent requirements may infrequently require the contractor to provide Service Desk Support on federal holidays and weekends (see paragraph 2.8).

1.8 WORK ENVIRONMENT AND HOURS OF OPERATION: Except as noted above, contractor personnel shall provide services between the hours of 0600 and 1800 Monday thru Friday with the exception of Federal holidays or when the Government facility is closed due to local or national emergencies, administrative closings, or similar Government directed facility closings. Contractor personnel may be required to participate in events which will fall outside of normal working hours. When such events occur, the Contractor PM Lead shall ensure individual contractor personnel work hours do not exceed 40 hours per work week.

Work is typically performed in an adequately lighted and climate controlled office space. Contractor personnel may be required to perform on afloat units, both in port and at-sea, and at the location of field exercises in support of the US Marine Corps. Contractor personnel may be required to conduct local, national and international travel in the performance of the contract.

At a minimum, contractor personnel filling the positions of Management Consultant, Director, Development Management, Web Applications Developer (all), Domino Administrator (all), Operations Specialist, Computer Operator, and Training Specialist will likely be required to perform aboard afloat units and during field exercises. At-sea periods are usually no more than two weeks in duration. When embarked aboard ships or operating in the field, contractor personnel may be exposed to adverse and hazardous conditions. At-sea assignments require physical exertion related to embarking, debarking and transferring to-and-from afloat commands and may include transit on Navy and USMC fixed, tilt-wing, and rotary-wing aircraft, support craft such as Landing Craft Air Cushioned (LCAC), Landing Craft Utility (LCU), Rigid Hull Inflatable Boats and TUGS supporting ship/shore and ship/ship personnel movement. All such assignments require the ability to stand for long periods, walk, climb, bend, crouch, stretch, reach above one's head and similar movements.

1.9 CONTRACTING OFFICER'S REPRESENTATIVE (COR): The (COR) will be identified by separate letter. The COR monitors all technical aspects of the contract and assists in contract administration. The COR is authorized to perform the following functions: assure that the Contractor performs the requirements of the contract: perform inspections necessary in connection with contract performance: maintain written and oral communications with the Contractor concerning various aspects of the contract: issue written interpretations of requirements: monitor Contractor's performance and notify both the Contracting Officer and Contractor of any deficiencies; coordinate availability of Government furnished property/training sites, and provide or coordinate site entry of Contractor personnel. A letter of designation issued to the COR, a copy of which is sent to the Contractor, states the responsibilities and limitations of the COR, especially with regard to changes in cost or price, estimates or changes in delivery dates. The COR is not authorized to change any of the terms and conditions of the resulting order.

1.10 IDENTIFICATION OF CONTRACTOR PERSONNEL: All contract personnel attending meetings, answering Government telephones, and working in other situations where their contractor status is not obvious to third parties are required to identify themselves as such to avoid creating an impression in the minds of members of the public that they are Government officials. They must also ensure that all

documents or reports produced by contractors are suitably marked as contractor products or that contractor participation is appropriately disclosed.

SECTION 2 CONTRACTOR TASKING

2.1 PERSONNEL: The contractor shall provide personnel with the position-dependent experience and certification(s) identified in Section 3.0.

2.2 PROGRAM MANAGEMENT SUPPORT: The Contractor shall designate a Contractor Program Management Support-lead (Contractor PM Lead) who shall be responsible for the performance of the tasking identified in Section 2 of this Performance Work Statement (PWS). The name of this person and an alternate who shall act for the contractor when the Contractor PM Lead is absent shall be designated in writing to the Contracting Officer and COR. The Contractor PM Lead or alternate shall have full authority to act for the contractor on all contract matters relating to daily operation of this contract. The Contractor PM Lead shall direct the effort of the contractor personnel and shall report and monitor progress to the NIDF Coalition and Allied Program Manager and COR through direct communication and the contract deliverables (Section 7).

The Contractor shall prepare briefings and presentations for flag/general officer and SES-level executives.

The Contractor shall provide Program Objective Memorandum (POM) preparation and analysis, strategic planning, acquisition planning and support, and proposal preparation and review support.

The Government and the Contractor shall jointly establish due dates specific to individual work products (ex., reports, course-related material, presentations, analysis, etc.) The Contractor shall provide progress reports on individual work products with assigned due dates in the Weekly Activity Report (paragraph 7.1)The Contractor shall coordinate and participate in Multinational Maritime IP Interoperability (M2I2) Steering Group meetings (with participating countries); IDFOR, Allied, and Coalition Interoperability Summits, secure releasable (SREL) (CENTRIXS), Cross Command and Technical Working group conferences, and other syndicates as required to support the Coalition and Allied Program.

The Contractor shall solicit, receive, input, and maintain the overall CAS/SREL (CENTRIXS) Program calendar and Weekly Activity Report.

The Contractor shall estimate and report on programmatic progress utilizing established milestones and deadlines for completion of assignments, projects, and tasks. The Contractor shall maintain awareness and participate in planning for achievement of team goals and objectives, research, learn, and apply a wide range of qualitative and/or quantitative methods to identify, assess, analyze and improve Navy coalition Command and Control (C2) effectiveness, efficiency, and work products.

The Contractor shall communicate recommendations on actions affecting the fleet, system products or progress.

2.3 DEVELOPMENT MANAGEMENT: The Contractor shall directly interface with the client related to CAS operations and maintenance within the SIPR, NIPR, and SREL CENTRIXS networks, validate CAS software versions and configurations, recommend software and hardware upgrades and enhancements, and conduct software development, testing, versioning, and deployment tasks.

The Contractor shall conduct technical reviews as required to ensure software modifications are meeting customer expectations. When required, the Contractor will participate in gathering, analyzing, and documenting customer requirements.

The Contractor shall provide inputs related to the development of the project management plan including investigation and analysis for determination of functional and performance requirements, maintenance on developed software and applications coding, project schedules and various planning, training and implementation tasks.

The Contractor shall coordinate and conduct quarterly Configuration Control Review Board (CCRB) meetings to obtain Government approval to work on recommended software changes and additions to the deployed CAS baseline.

The Contractor shall establish programmatic processes and procedures by drafting, implementing, and maintaining Standard Operating procedures (SOPs); standardized documents such as User Guides, Test Plans, Configuration Guides, and training plans.

2.4 OPERATIONS SUPPORT: The Contractor shall provide Subject Matter Expertise and technical support to assist in solving issues or completing specific tasks related to support SREL (CENTRIXS) and CAS software and hardware architecture. This may include, but is not limited to, system hardware and software programming updates, modifications, troubleshooting, debugging, interface management, network analysis, system security, technical and engineering documentation, and system administration, configuration, and testing.

The Contractor shall provide expert technical advice and guidance to Government entities concerning Coalition Information Technology (IT) Systems.

The Contractor shall assist in the formulation and analysis of overall IT information systems objectives. The Contractor shall make recommendations on technical direction and policy structure and oversight for IT programs, innovation projects and readiness support for local area networks for all operating units and shore support activities using coalition communication systems.

The Contractor shall provide input for planning and coordinating implementation of technical IT capabilities, hardware and software, to meet existing and future Coalition/Allied system requirements. The Contractor shall recommend alternatives to support planning and development of programs relative to information systems, data exchange and transfer and LAN capabilities for the integration and implementation of Readiness Assessment and Decision Support Systems.

The Contractor shall monitor activities designing and/or specifying design criteria for systems to remain knowledgeable of technological change and its impact on other systems and personnel. The Contactor shall assess the suitability, technical excellence, acceptability and relevance of proposals.

2.5 SYSTEMS ENGINEERING SUPPORT: The Contractor shall perform systems engineering functions to include developing functional requirements and objectives for software and hardware products for the Coalition Systems Division.

The Contractor shall provide technical advice and consultation to systems analysts, programmers and functional managers on the subjects of system configuration alternatives (hardware, software, firmware, network, and interfaces); system capabilities and problem resolution and system utilities.

The Contractor shall monitor system development, testing and implementation, and conduct evaluations of existing command support systems to determine performance adequacy and usability.

The Contractor shall monitor the development of technical solutions for problems through the use of information technology venues. The Contractor shall plan work in support of operational units in the areas of Combat, Command and Control, and Tactical Support.

The Contractor shall provide support for the operation and maintenance of the Unified Atlantic Region Network Operations Center (UARNOC), Pacific Region Network Operations Center (PRNOC), Maritime Operations Center's (MOC's) and Fleet CAS SIPR, NIPR, and SREL (CENTRIXS) networks hardware and software.

The Contractor shall provide services which include, but not limited to, user and server administrative support functions, service desk functions (Tiers I through III), Information Assurance (IA) support, IAVA

compliance, database and network administration, including installation of hardware and software product upgrades, operational support, and systems configuration, maintenance, and testing.

The Contractor shall provide technical support as related to operational support for the UARNOC and PRNOC CAS SIPR, CAS NIPR, and SREL (CENTRIXS) networks.

The Contractor shall maintain expertise on hardware, software, LANs, and computer technology required to support CAS and SREL (CENTRIXS) hardware and software.

The Contractor shall provide systems administration services.

2.6 INFORMATION ASSURANCE: The Contractor shall provide support to maintain the system, network, and application security for the CAS SIPR, NIPR and CENTRIXS implementations, including managing and updating the DoD Information Assurance Certification and Accreditation Process (DIACAP) package. The support shall include, but is not limited to, the development and updating of the DIACAP Implementation Plan (DIP), System Identification Plan (SIP), and all necessary artifacts as required by the Navy Operational Designated Accreditation Authority (ODAA).

The Contractor shall conduct applicable scanning, as specified by the Navy ODAA and performing mitigating actions for CAS NIPR, SIPR, and CENTRIXS production and non-production networks to comply with these requirements.

The Contractor shall support the integration of all CAS SIPR and NIPR, standalone network Information Assurance Vulnerability Alerts (IAVA) compliances.

The contractor shall update CAS system IATOs or ATOs as required.

2.7 NETWORK SECURITY: The Contractor shall provide network security services including research, evaluation, design, implementation, administration, monitoring, support, and maintenance of CAS SIPR, NIPR, and SREL (CENTRIXS) network hardware and software systems.

The Contractor shall be familiar with CAS SIPR, NIPR, and SREL (CENTRIXS) networks, systems, and the management and control of these systems, including network architecture, interfaces, software and functional requirements.

The Contractor shall review requirements, design solutions, and implement security and systems administration procedures to set up new networks or modify existing networks.

2.8 SERVICE DESK SUPPORT: The Contractor shall provide tier I through III Service Desk support to U.S. and Coalition/Allied users. The Contractor shall staff and manage the UARNOC and PRNOC Service Desks.

The Contractor shall provide real-time support of UARNOC and PRNOC watch operations, supporting deployed ships and shore based CAS and SREL (CENTRIXS) users via telephone, chat services, Fleet Web Support, and email.

As part of the Service Desk tasking, the Contractor shall provide system deployment and upgrade support for scheduled CAS and SREL (CENTRIXS) installations.

2.8.1 UARNOC: The UARNOC Service Desk shall be staffed from 0600-1800 EST Monday through Friday. Service Desk activities are a collateral duty for personnel assigned to the UARNOC.

The UARNOC Service Desk may require staffing outside of normal working hours due to real-world operations, testing, or at other times set by UARNOC CIO and Deputy CIO, in coordination with the Contactor PM Lead, and may include weekends and federal holidays. During these times, the Contractor shall develop a watch-standing schedule to ensure Service Desk coverage. The Contractor shall ensure individual contract employee work-hours do not exceed 40 hours per week.

2.8.2 PRNOC: The PRNOC Service Desk shall be staffed from 0600-2300 HST, seven days a week, 365 days a year.

The PRNOC Service Desk may require staffing outside of normal working hours (2300 -0600) due to real-world operations, testing, or at other times set by PRNOC Operations Officer and Technical Director, in coordination with the Contractor PM Lead. During these times, the Contractor shall develop a watch-standing schedule to ensure Service Desk coverage. The Contractor shall ensure individual contract employee work-hours do not exceed 40 hours per week.

2.9 WEB APPLICATION DEVELOPMENT: The Contractor shall gather and analyze user requirements, develop new software modules and modify existing software modules following government approval. Software modules shall be modified by the Contractor outside of the quarterly build process when critical bugs are identified.

The Contractor shall provide on-site tutoring to operational sites (tactical units) to increase user-level knowledge of site configuration options, posting options, best practices of CAS uses, and to collect user requirements for the quarterly update cycle.

The Contractor shall develop assigned web applications for the CAS/SREL (CENTRIXS) environment that are compatible with all releasable enclaves.

The Contractor shall develop web applications to validated user requirements, providing fully tested and documented web applications and web services to the Fleet.

2.9.1 Web Application Testing: Following web application development, the Contractor shall conduct internal testing of CAS modules to ensure code changes work internal to the module prior to performing functional testing. Internal testing will be performed on unclassified websites located at the UARNOC, PRNOC, and/or off-site Government data centers. The Contractor shall perform functional testing on the Functional Test Network (FTN) which replicates the deployed versions of CAS operating on server and software loads encountered in the deployed CAS/SREL (CENTRIXS) environments.

The Contractor shall maintain the FTN that possesses these loads for use during functional testing.

The Contractor shall maintain web sites.

2.9.2 Versioning: Versioning will be performed by the Contractor following successful testing.

2.9.3 Module Deployment: The Contractor shall schedule and deploy all modules onto the SIPR CAS enclave as approved by the Government. Following successful deployment across the SIPR CAS enclave, the Contractor shall deploy modules onto the remaining SREL (CENTRIXS) enclaves to maintain configuration control.

2.10 TECHNICAL WRITING: The Contractor shall perform a full range of technical writing tasks in support of the Coalition and Allied Program by developing or modifying CAS module Test Plans and Configuration Guides in support of module testing activities.

The Contractor shall develop or modify CAS module User Guides in support of the web development process prior to deploying completed modules across enclaves.

The Contractor shall create, update, and use separate versioned websites residing on a NIPR network at an off-site Government run data center to document and verify Test Plans, User Guides, and Configuration Guides prior to software modules entering into the functional testing, integration testing, versioning, and deployment phases.

The Contractor shall maintain configuration control of all documentation using an established web based CAS documentation database on the CAS NIPR network.

The Contractor shall draft, edit, and proofread Standard Operating Procedures (SOP's) and documenting processes and procedures of the CAS program, and maintain the latest versions of documents within the

CAS documentation database. When required, the Contractor shall participate in gathering, analyzing, and documenting customer requirements. This work may be performed at Government-approved telework sites.

2.11 ON-SITE TRAINING AND SUPPORT: The Contractor shall provide technical support, curricula development, training execution, and exercise support for SREL (CENTRIXS) and or Collaboration at Sea in accordance with objectives outlined by NIDF, SPAWAR, COMLANTFLT, and COMPACFLT.

The Contractor shall provide commercial off-the-shelf (COTS) product integration, installation and operational support to the current SREL (CENTRIXS) architecture to support existing security enclaves and the extension of SREL (CENTRIXS) to other Coalition Partner enclaves, as directed by IDFOR.

The Contractor shall review on-site design for SREL (CENTRIXS) and coalition network support configurations in cooperation with the Navy Network Operations Centers (NOCs), develop communications training curricula for SREL (CENTRIXS) and CAS operators and system administrators and conduct training for specific customers, and facilitate the development of electronic learning tools that complement written documentation.

To ensure connectivity across enclaves with coalition partners, the Contractor shall provide consistent support for exercises, demonstrations, and evaluations where SREL (CENTRIXS) and or Collaboration at Sea are principle components.

SECTION 3 POSITIONS, LABOR CATEGORIES and QUALIFICATIONS

3.1 POSITIONS: The position titles, estimated number of full-time (40 hours per week) contractor personnel and the principal place of performance locations are identified below. Positions listed without a performance location designated may be performed in the Tidewater, VA area or Honolulu, HI area. Cybersecurity Workforce (CSWF), Information Assurance Manager (IAM) and Information Assurance Technical (IAT) positions and descriptions can be found in reference c., Information Assurance (IA) Workforce Improvement Program.

TITLE	LEVEL	EST NUMBER OF PERS	LOCATION
Contractor Program Manager Lead (KEY)		1	Tidewater, VA area
Management Consultant Coalition Systems		1	Tidewater, VA area
Director, Development Management	SME 5 (CSWF IAT I/II)	1	Tidewater, VA area
Web Applications Developer	SME 5 (CSWF IAT II/III)	1	
Web Applications Developer	SME 4 (CSWF IAT II/III)	2	
Web Applications Developer	SME 2 (CSWF IAT II/III)	1	Tidewater, VA area
Domino Administrator	SME 3 (CSWF IAT II/III)	5	Norfolk, VA
Domino Administrator	SME 3 (CSWF IAT II/III)	5	Honolulu, HI area
SCA Computer Operator	Lvl V (CSWF IAT I/II)	1	Tidewater, VA area
SCA Computer Operator	Lvl V (CSWF IAT I/II)	1	Honolulu, HI area
Training Specialist (CAS/SREL)	Training Specialist 3 (CSWF IAT I/II)	3	Tidewater, VA area
Operations Specialist	(CSWF IAT I/II)	1	Tidewater, VA area
Technical Writer/Editor	Technical Writer/Editor 3	1	

The Government anticipates Task Order 0001 will be issued soon after contract award to fill the contractor positions of Program Manager Lead, Web Applications Developer (SME 5), Web Applications Developer (SME 4), all Domino Administrators (SME 3), and Technical Writer/Editor (Lvl 3).

3.2 MINIMUM PERSONNEL QUALIFICATIONS: Personnel utilized by the Contractor in the performance of this contract shall, at a minimum, meet the position-based experience, education, or other background requirements set forth below and shall be fully capable of performing in an efficient, reliable, and professional manner. In addition to the stated minimum qualifications, all Contractor personnel performing Information Assurance (IA) (Cybersecurity Workforce/Information Assurance Work Force (CSWF/IAWF)) functions shall meet the training and certification requirements contained in DOD Directive 8570.1M titled Information Assurance Training, Certification, and Workforce Management. Contractor personnel shall be appropriately certified prior to reporting, no exceptions.

The Government reserves the right to review the resume and request validation of certifications and experience of contractor staff designated as Key Personnel.

3.3 CONTRACTOR PROGRAM MANAGER SUPPORT LEAD (Key Personnel):

Education: Bachelor of Science degree in Computer Science, Information Systems, or other Engineering discipline required. A Master's of Science in Computer Science, Information Systems, or other Engineering discipline strongly desired.

Experience: The Contractor Program Manager Support Lead shall have a minimum of seven (7) years practical experience at a professional level in Information Technology (IT) Systems / Information Operations (IO) within or supporting the Department of Defense. Additional experience shall include the following (which may be gained concurrently): Seven (7) years of experience managing complex projects or programs; successful performance at the program management-level, with responsibility for management and control of cost, schedule, performance, and personnel, and communicating/interfacing with customers on tasking similar to what is described in Section 2 of the PWS. Knowledge of Federal Acquisition Regulation (FAR) and DoD procurement policies and procedures; preparing and delivering briefs; and drafting documents to high level audiences (O-6/GS-15 level and above).

Clearance: SECRET

3.4 MANAGEMENT CONSULTANT COALITION SYSTEMS:

Education: Bachelor of Science degree in Computer Science, Information Systems, or other Engineering discipline required. Minimum of two (2) years of relevant experience in lieu of each year of formal education may be substituted for a formal degree.

Experience: Fifteen (15) years of experience managing progressively more complex and/or multiple technical programs/projects with responsibility for management and control of cost, schedule, performance, and personnel, communicating and interfacing with customers for work elements similar to those described in the PWS. Eight (8) years Program Management experience, to include: Information Assurance/Information Security; System requirements analysis, System Test and Evaluation, planning and execution; Software requirements analysis, design, integration, development, application and testing; Program management, project management and product milestone scheduling for technical development; Logistics and configuration management planning, development and implementation. Knowledge of Federal Acquisition Regulation (FAR) and DoD procurement policies and procedures.

Clearance: SECRET

3.5 DIRECTOR, DEVELOPMENT MANAGEMENT, SME 5:

Education: Bachelor of Science degree in Computer Science, Information Systems, or other Engineering discipline required. A Master's of Science in Computer Science, Information Systems, or other Engineering discipline strongly desired.

Experience: Ten (10) years of experience managing progressively more complex and/or multiple technical programs/projects and responsible for management and control of cost, schedules, performance, and personnel, communicating and interfacing with customers for tasks similar to those described in the PWS. Eight (8) years of technical experience in the operation, maintenance, engineering, testing, training, and program management support of C4ISR systems and experience providing overall direction of project activities within a DOD or government acquisition program structure. Eight (8) years of experience in the following: Knowledge of Federal Acquisition Regulation (FAR) and DoD procurement policies and procedures; preparing and delivering briefs; and drafting documents to high level audiences (O-6/GS-15 level and above). Knowledge of FAR and DoD procurement policies and procedures.

Certifications: Comply with the certification requirements based on DoDI 8570 IAT-I/II requirements.

Clearance: SECRET

3.6 WEB APPLICATIONS DEVELOPER:

Education: Bachelor of Science degree in Computer Science, Information Systems, or other Engineering discipline required. Minimum of two (2) years of relevant experience in lieu of each year of formal education may be substituted for a formal degree. Highly desire a Lotus Developer Certification (version 6 or higher).

Experience:

SME 2: Two (2) years of experience providing Lotus Domino web development support in a web-based, distributed environment, including the ability to design, code, test and implement custom web applications by utilizing and applying a broad knowledge of programming languages to include Lotus Script, Java, Java Script, AJAX, HTML, DHTML, and XML and process documentation to support software development. One (1) year of formal education may be substituted for two (2) years of this relevant experience. Experience versioning software working with TeamStudio CIAO! and TeamStudio Delta or similar software (SourceSafe, CVS, etc.).

SME 4: Seven (7) years of experience providing Lotus Domino web development support in a web-based, distributed environment, including the ability to design, code, test and implement custom web applications by utilizing and applying a broad knowledge of programming languages to include Lotus Script, Java, Java Script, AJAX, HTML, DHTML, and XML and process documentation to support software development. One (1) year of formal education may be substituted for two (2) years of this relevant experience. Experience versioning software working with TeamStudio CIAO! and TeamStudio Delta or similar software (SourceSafe, CVS, etc.).

SME 5: Ten (10) years of experience providing Lotus Domino web development support in a web-based, distributed environment, including the ability to design, code, test and implement custom web applications by utilizing and applying a broad knowledge of programming languages to include Lotus Script, Java, Java Script, AJAX, HTML, DHTML, and XML and process documentation to support software development. One (1) year of formal education may be substituted for two (2) years of this relevant experience. Experience versioning software working with TeamStudio CIAO! and TeamStudio Delta or similar software (SourceSafe, CVS, etc.).

Certifications (all): SECURITY + and OS certification required, comply with the certification requirements based on DoDI 8570 IAT-II/III requirements. Highly desire a Lotus Developer Certification version 6 or higher.

Clearance: TOP SECRET/SCI clearance is required for those positions in Hawaii; SECRET clearance is required for the positions in the Tidewater, VA area.

3.7 LOTUS DOMINO SYSTEMS ADMINISTRATOR, SME 3:

Education: Bachelor of Science degree in Computer Science, Information Systems, or other Engineering discipline required. Minimum of two (2) years of relevant experience in lieu of each year of formal education may be substituted for a formal degree.

Experience: Four (4) years of experience providing Lotus Domino Systems Administrator service desk services Tiers I, II, and III across a variety of hardware platforms and software programs. One (1) year of formal education may be substituted for two (2) years of this relevant experience. Seven (7) years of demonstrated experience working with Windows Server; MS Office, Symantec Endpoint, and third party tools such as ACAS, Retina CS, Server AdminPlus and GSX. Demonstrated experience performing Information Assurance (IA) security procedures, which may include scanning and mitigating actions. Experience working with TeamStudio CIAO! and TeamStudio Delta or similar software (SourceSafe, CVS, etc.). Demonstrated experience in a software testing environment.

Certifications: SECURITY + and OS certification required, comply with the certification requirements based on DoDI 8570 IAT-II/III requirements.

Clearance: TOP SECRET/SCI clearance is required for the positions in Hawaii; SECRET clearance is required for the positions at the UARNOC. Positions at UARNOC may require a TOP SECRET/SCI clearance at some future point.

3.8 SCA COMPUTER OPERATOR, LEVEL V:

Experience: A minimum of (3) years of work experience in the area of computer operations of which (2) years must be specialized experience operating a large-scale multi-server local area network. Experience working with TeamStudio CIAO! and TeamStudio Delta or similar software (SourceSafe, CVS, etc.).

Certifications: SECURITY + and OS certification required, comply with the certification requirements based on DoDI 8570 IAT-I/II requirements.

Clearance: One position will require a **TOP SECRET/SCI** (PRNOC) clearance and the other a **SECRET** (UARNOC). The SECRET clearance requirement at some point may be required to upgrade to a **TOP SECRET/SCI**.

3.9 TRAINING SPECIALIST, LEVEL 3:

Education: Bachelor of Science degree in Information Technology, Computer Science or other scientific field. Minimum of two (2) years of relevant experience in lieu of each year of formal education may be substituted for a formal degree.

Experience: Must possess recent and relevant experience with Fleet communications, CAS, and CENTRIXS systems. Must be familiar with CAS/CENTRIXS hardware to include a demonstrated proficiency in the operation and maintenance of servers, PC's, crypto-logic devices, hubs, and switches. Must be familiar with CAS/CENTRIXS software to include Windows Server 2008, 2012; MS Office, Symantec Endpoint, and third party tools such as Server AdminPlus and GSX. Must be familiar with the CAS (Lotus Domino) Program, Sametime Chat, Persistent Chat, Domino web mail, and Microsoft Exchange Based e-mail to provide effective training. Must possess excellent communication skills in a class room training environment.

Certifications: SECURITY + and OS certification required, comply with the certification requirements based on DoDI 8570 IAT-I/II requirements.

Clearance: SECRET - at some point may be required to upgrade to a **TOP SECRET/SCI.**

3.10 OPERATIONS SPECIALIST:

Education: Bachelor of Science degree in Computer Science, Information Systems, or other Engineering discipline required. Minimum of two (2) years of relevant experience in lieu of each year of formal education may be substituted for a formal degree.

Experience: Four (4) or more years of experience in the U.S. Navy serving on operational, combatant commander or joint staffs (Strike Group, Expeditionary Ready Group, Fleet Command, Regional Command, etc…) at the E-8 paygrade or higher. Must have four (4) or more years of experience participating in high level Joint and Coalition exercises. Must possess relevant experience associated with planning requirements for real world operations. Demonstrated experience using MS Word and MS Power Point software preparing briefings and white papers.

Certifications: SECURITY + certification required, comply with the certification requirements based on DoDI 8570 IAT-I/II requirements.

Clearance: SECRET

3.8 TECHNICAL WRITER, LEVEL 3:

Education: Bachelor's degree in any physical science, English or Journalism curriculum. Minimum of two (2) years of relevant experience in lieu of each year of formal education may be substituted for a formal degree.

Experience: Four (4) years of experience in the preparation of Department of Defense documents related to the Procurement/Integrated Logistic Support/instruction manuals/system, specifications, SOPs, Military Standards, software program test plans, configuration guides, administrative guides, and user guides. Experience using MS Word software, Visio Drawing software, Adobe Acrobat software, and MS Power Point software. Experience using and documenting code in software programs written in Lotus Script, Java, Java Script, AJAX, HTML, DHTML, and XML languages. Possess knowledge of the Government Printing Office Style Manual.

Clearance: SECRET

SECTION 4 QUALITY ASSURANCE

4.1 CONTRACTOR QUALITY ASSURANCE: The contractor shall develop and maintain a Quality Assurance Plan (QA Plan) in order to ensure only qualified personnel, as stipulated in Section 3, are assigned to fulfill the requirements stated in this PWS. The contractor shall detail in its quality assurance plan how it intends to maintain personnel qualifications and ensure contract employees have up-to-date training and knowledge in their respective areas of endeavor.

This QA Plan shall detail the methodology to be used by the contractor to monitor and grade the performance of its personnel as they carry out the requirements of this PWS. The QA Plan shall address the contractor's courses of action to address under-performing employees.

4.2 GOVERNMENT QUALITY ASSURANCE SURVEILLANCE: The Government shall evaluate the contractor's performance under this contract in accordance with the Quality Assurance Surveillance Plan (QASP). This plan is primarily focused on what the Government must do in order to ensure that the contractor is performing in accordance with the performance standards. It defines how the performance standards will be applied, the frequency of surveillance, and the minimum acceptable defect rate(s).

SECTION 5 SECURITY

5.1 ACCESS TO GOVERNMENT FACILITIES: Access will be granted to Government facilities as required in support of the tasking. Contractor personnel performing work under this contract must meet all requirements for gaining access to US Government installations. The contractor shall conform to all DoD, DoN, and local (base/installation) security instructions (refer to **Contractor Unclassified Access to Federally Controlled Facilities, Sensitive Information, Information Technology (IT) Systems or Protected Health Information (July 2013)** provided below).

5.2 SECURITY CLEARANCES: The highest level of security clearance required under this contract is **TOP SECRET/SCI**, as required by individual tasking orders and as designated on the standard DD Form 254. The Contractor is responsible for acquiring and maintaining security clearances at the appropriate level(s) under this contract.

5.3 VISIT REQUESTS: Request for visit authorizations by Contractors when security access is required shall be submitted to the address listed below in accordance with Department of Defense (DOD) 5220.22M National Industrial Security Program Operating Manual (NISPOM) not later than one week prior to visit for certification of need-to-know by the specified Contracting Officer's Representative (COR)/Task Order Manager (TOM). DD-254 of the basic contract applies.

Requests shall be forwarded to the **NAVIDFOR Special Security Office (SSO), Attn: Security Office**

5.4 COMMON ACCESS CARD (CAC): The Government Contractor CAC card serves as the primary method of identification for the contractor employees, as well as providing the basis of Public Key Infrastructure (PKI) access to the Navy/Marine Corps Intranet (NMCI), and numerous Navy web sites, which may also require PKI access. The COR shall assist in providing the contractor the appropriate documentation for obtaining CAC cards.

The Contractor shall be responsible for obtaining any Government issued identification cards from former employees or employees whose access has been terminated and to turn those items over to the Command Security Officer upon termination of employment or access.

SECTION 6 OTHER DIRECT COSTS

6.1 TRAVEL**:** The contractor shall be required to travel in the performance of the tasking detailed in this PWS. Travel costs for transportation, lodging, meals and incidental expenses are allowable if incurred by contractor personnel on official business. Travel related costs shall be reasonable. Costs for transportation may be based on mileage rates, actual costs incurred, or a combination thereof, provided the method used results in a reasonable charge. Costs incurred for lodging, meals and incidental expenses shall be considered reasonable and allowable only to the extent they do not exceed on a daily basis the maximum per diem rates in effect at the time of travel. See FAR 31.205-46 for more information on travel costs. Travel costs are further limited by funds specified in the contract.

The Contractor shall submit a request, via email, to the COR seeking approval to deviate from the trips listed in the table below before initiating any travel plans. All travel claims shall make reference to this PWS, e-mail, letter or phone call from the Government that granted approval. Failure to gain prior approval may result in disallowance of invoiced travel claims. For travel to foreign countries, the contractor personnel must meet the travel requirements, to include training requirements, established for the respective Area of Responsibility (AOR). Country-specific Status of Forces Agreement (SOFA) is provided in at the end of this PWS for informational purposes only. Contractor shall research the most current rules, regulations, policies, restrictions, etc., prior to travel. The following itemized trips are anticipated during the first year of this contract in each option year.

Origination/Destination	**# of Trips**	**# of Travelers**	**Duration (Days)**
Suffolk, VA/Portsmouth, UK	1	2	5
Suffolk, VA/Portsmouth, UK	**1**	**1**	**7**
Honolulu, HI/Portsmouth, UK	**1**	**2**	**5**
Suffolk, VA/Honolulu, HI	**1**	**3**	**5**
Suffolk, VA/Honolulu, HI	**1**	**2**	**5**
Suffolk, VA/Honolulu, HI	**2**	**1**	**7**
Suffolk, VA/Honolulu, HI	**4**	**1**	**5**
Suffolk, VA/San Diego, CA	**2**	**4**	**5**
Suffolk, VA/San Diego, CA	**5**	**1**	**7**
Honolulu, HI/San Diego, CA	**2**	**4**	**5**
Honolulu, HI/Suffolk, VA	**2**	**1**	**5**
Suffolk, VA/Washington, DC	**4**	**1**	**5**
Suffolk, VA/Yokosuka, Japan	**2**	**2**	**14**
Suffolk, VA/Everett/Bremerton, WA	**2**	**1**	**5**
Suffolk, VA/Sydney, AU	**1**	**3**	**7**
Suffolk, VA/Sydney, AU	**1**	**1**	**5**
Suffolk, VA/Tampa Bay, FL	**1**	**1**	**5**
Suffolk, VA/Mayport, FL	**5**	**1**	**5**

Suffolk, VA/Berlin, DEU	**1**	**3**	**7**
Suffolk, VA/Bahrain	**1**	**2**	**10**
Suffolk, VA/Naples, Italy	**1**	**2**	**7**
Suffolk, VA/Rio De Janeiro, Brazil	**1**	**5**	**5**

6.2 CONSUMABLE ITEMS: With prior approval from the COR, the Contractor may procure material which is not readily or quickly available and necessary to support urgent requirements. The exact material requirements are not definable; however, the need for the Contractor to procure items is expected to be infrequent with annual expenditures below the DOD micro-purchase limit of $3,000. Consumable items might include various cable, adaptors, connectors, nuts, bolts, tape stock, and similar items. All IT related procurements must comply with the Department of Defense (DOD) and Department of Navy (DON) statutory and regulatory requirements.

SECTION 7 CONTRACT DELIVERABLES

7.1 WEEKLY ACTIVITY REPORT: The Weekly Activity Report shall be submitted not later than 5 business days after end of the week reported on. The report shall contain the following information at a minimum:

a. Task status (include originator/customer, personnel assigned to complete, location, goal/end-state, estimated completion date, percent complete)

b. Tasks completed (date completed)

c. Issues impacting milestone attainment

d. Personnel issues

e. Upcoming Events

7.2 MONTHLY STATUS REPORT: The Monthly Status Report shall be submitted not later than 15 business days after end of the month reported on. The report shall contain the following information at a minimum:

a. Tasks completed during the reporting period

b. Personnel issues

c. Upcoming Travel

d. Named operations and exercises supported

e. U.S. and coalition commands supported

f. Software development status

g. Anticipated activity for next reporting period

7.3 TRIP REPORT The contractor shall require his/her employees to file a trip report upon return from any periods of travel. The trip report shall be in a format prescribed by the contractor, but at a minimum, shall address the objectives of the travel and whether those objectives were or were not achieved. If not achieved, the circumstances preventing the accomplishment of the objective shall also be provided. Upon submission, a copy shall be provided to the COR.

7.4 MONTHLY FINANCIAL REPORT: The Monthly Financial Report shall be submitted not later than 10 business days after end of the month reported on. The report shall contain the following information at a minimum:

a. Current month travel expenses per trip and contract to date travel expense

b. Current month and contract to date for non-travel other direct costs expensed

c. Invoices submitted but not paid

Deliverable Product Format: All reports and documentation will be developed using recent versions of Adobe Acrobat, Microsoft Office Professional Products to include Word, Excel, PowerPoint, etc.

SECTION 8 MISCELLANEOUS

8.1 COMPLAINTS LODGED AGAINST CONTRACTOR PERSONNEL: In the event that a complaint is made regarding the conduct or ability of contractor personnel, the individual receiving the complaint will contact the COR. The COR will notify the Contractor PM Lead. The Contract PM Lead and COR will cooperate in investigating complaints made against contractor employees. If the results of the investigation prove the complaint(s) to be valid, the Contractor PM Lead shall have a maximum of three (3) working days to propose a corrective plan for resolving the matter and preventing future similar occurrences. This plan shall be submitted in writing to the Contracting Officer and COR. In the event that the Government deems the corrective plan insufficient for resolution of the problem, a written response to the Contractor Manager shall be provided within three (3) working days.

8.2 GOVERNMENT FURNISHED INFORMATION: GFI will be provided to contractor employees as needed to complete the tasks set forth in this performance work statement. Access to classified information must be granted in accordance with the terms and conditions contained in DOD Manual 5220.22-M and DD Form 254 (Contract Security Classification Specification).

8.3 OFFICE SPACE: Government will provide office space at the respective locations. In addition to office space, each contract employees shall be provided with access to government computers and telephones, but not cellular phones, for official use only. Under no circumstances will contractor-provided personal computers will be connected to the Navy/Marine Corps Intranet (NMCI). Contractor personnel shall comply with all DOD and Navy internet usage and cybersecurity policies.

8.4 STATEMENT OF NON-PERSONAL SERVICE: Contractor employees performing services under this contract will be controlled, directed, and supervised at all times by management personnel of the contractor. Contractor management shall ensure that employees properly comply with the performance work standards outlined in the PWS. Contractor employees shall perform their duties independent of, and without the supervision of, any Government official. The tasks, duties, and responsibilities set forth in this contract shall not be interpreted or implemented in any manner that results in any contractor employee creating or modifying Federal policy, obligating the appropriated funds of the United States Government, overseeing the work of Federal employees, providing direct personal services to any Federal employee, or otherwise violating the prohibitions set forth in Parts 7.5 and 37.1 of the Federal Acquisition Regulation (FAR) http://farsite.hill.af.mil/vffar1.htm . The Government shall control access to the facilities and shall perform the inspection and acceptance of completed work.

8.7 INVOICING: Invoices shall be submitted via the Wide Area Workflow system.

Contractor Unclassified Access to Federally Controlled Facilities, Sensitive Information, Information Technology (IT) Systems or Protected Health Information
(July 2013)

Homeland Security Presidential Directive (HSPD)-12, requires government agencies to develop and implement Federal security standards for Federal employees and contractors. The Deputy Secretary of Defense Directive-Type Memorandum (DTM) 08-006 – "DoD Implementation of Homeland Security Presidential Directive – 12 (HSPD-12)" dated November 26, 2008 (or its subsequent DoD instruction) directs implementation of HSPD-12. This clause is in accordance with HSPD-12 and its implementing directives.

APPLICABILITY
This clause applies to contractor employees requiring physical access to any area of a federally controlled base, facility or activity and/or requiring access to a DoN or DoD computer/network/system to perform certain unclassified sensitive duties. This clause also applies to contractor employees who access Privacy Act and Protected Health Information, provide support associated with fiduciary duties, or perform duties that have been identified by DON as National Security Position, as advised by the command security manager. It is the responsibility of the responsible security officer of the command/facility where the work is performed to ensure compliance.

Each contractor employee providing services at a Navy Command under this contract is required to obtain a Department of Defense Common Access Card (DoD CAC). Additionally, depending on the level of computer/network access, the contract employee will require a successful investigation as detailed below.

ACCESS TO FEDERAL FACILITIES
Per HSPD-12 and implementing guidance, all contractor employees working at a federally controlled base, facility or activity under this clause will require a DoD CAC. When access to a base, facility or activity is required contractor employees shall in-process with the Navy Command's Security Manager upon arrival to the Navy Command and shall out-process prior to their departure at the completion of the individual's performance under the contract.

ACCESS TO DOD IT SYSTEMS
In accordance with SECNAV M-5510.30, contractor employees who require access to DoN or DoD networks are categorized as IT-I, IT-II, or IT-III. The IT-II level, defined in detail in SECNAV M-5510.30, includes positions which require access to information protected under the Privacy Act, to include Protected Health Information (PHI). All contractor employees under this contract who require access to Privacy Act protected information are therefore categorized no lower than IT-II. IT Levels are determined by the requiring activity's Command Information Assurance Manager. Contractor employees requiring privileged or IT-I level access, (when specified by the terms of the contract) require a Single Scope Background Investigation (SSBI) which is a higher level investigation than the National Agency Check with Law and Credit (NACLC) described below. Due to the privileged system access, a SSBI suitable for High Risk public trusts positions is required. Individuals who have access to system control, monitoring, or administration functions (e.g. system administrator, database administrator) require training and certification to Information Assurance Technical Level 1, and must be trained and certified on the Operating System or Computing Environment they are required to maintain.

Access to sensitive IT systems is contingent upon a favorably adjudicated background investigation. When access to IT systems is required for performance of the contractor employee's duties, such employees shall in-process with the Navy Command's Security Manager and Information Assurance Manager upon arrival to the Navy command and shall out-process prior to their departure at the completion of the individual's performance under the contract. Completion and approval of a System Authorization Access Request Navy (SAAR-N) form is required for all individuals accessing Navy Information Technology resources. The decision to authorize access to a government IT system/network is inherently governmental. The contractor supervisor is not authorized to sign the SAAR-N; therefore, the government employee with knowledge of the system/network access required or the COR shall sign the SAAR-N as the "supervisor".

The SAAR-N shall be forwarded to the Navy Command's Security Manager at least 30 days prior to the individual's start date. Failure to provide the required documentation at least 30 days prior to the individual's start date may result in delaying the individual's start date.

When required to maintain access to required IT systems or networks, the contractor shall ensure that all employees requiring access complete annual Information Assurance (IA) training, and maintain a current requisite background investigation. The Contractor's Security Representative shall contact the Command Security Manager for guidance when reinvestigations are required.

INTERIM ACCESS
The Navy Command's Security Manager may authorize issuance of a DoD CAC and interim access to a DoN or DoD unclassified computer/network upon a favorable review of the investigative questionnaire and advance favorable fingerprint results. When the results of the investigation are received and a favorable determination is not made, the contractor employee working on the contract under interim access will be denied access to the computer network and this denial will not relieve the contractor of his/her responsibility to perform.

DENIAL OR TERMINATION OF ACCESS
The potential consequences of any requirement under this clause including denial or termination of physical or system access in no way relieves the contractor from the requirement to execute performance under the contract within the timeframes specified in the contract. Contractors shall plan ahead in processing their employees and subcontractor employees. The contractor shall insert this clause in all subcontracts when the subcontractor is permitted to have unclassified access to a federally controlled facility, federally-controlled information system/network and/or to government information, meaning information not authorized for public release.

CONTRACTOR'S SECURITY REPRESENTATIVE
The contractor shall designate an employee to serve as the Contractor's Security Representative. Within three work days after contract award, the contractor shall provide to the requiring activity's Security Manager and the Contracting Officer, in writing, the name, title, address and phone number for the Contractor's Security Representative. The Contractor's Security Representative shall be the primary point of contact on any security matter. The Contractor's Security Representative shall not be replaced or removed without prior notice to the Contracting Officer and Command Security Manager.

BACKGROUND INVESTIGATION REQUIREMENTS AND SECURITY APPROVAL PROCESS FOR CONTRACTORS ASSIGNED TO NATIONAL SECURITY POSITIONS OR PERFORMING SENSITIVE DUTIES
Navy security policy requires that all positions be given a sensitivity value based on level of risk factors to ensure appropriate protective measures are applied. Navy recognizes contractor employees under this contract as Non-Critical Sensitive [ADP/IT-II] when the contract scope of work require physical access to a federally controlled base, facility or activity and/or requiring access to a DoD computer/network, to perform unclassified sensitive duties. This designation is also applied to contractor employees who access Privacy Act and Protected Health Information (PHI), provide support associated with fiduciary duties, or perform duties that have been identified by DON as National Security Positions. At a minimum, each contractor employee must be a US citizen and have a favorably completed NACLC to obtain a favorable determination for assignment to a non-critical sensitive or IT-II position. The NACLC consists of a standard NAC and a FBI fingerprint check plus law enforcement checks and credit check. Each contractor employee filling a non-critical sensitive or IT-II position is required to complete:

- SF-86 Questionnaire for National Security Positions (or equivalent OPM investigative product)
- Two FD-258 Applicant Fingerprint Cards (or an electronic fingerprint submission)
- Original Signed Release Statements

Failure to provide the required documentation at least 30 days prior to the individual's start date shall result in delaying the individual's start date. Background investigations shall be reinitiated as required to ensure investigations remain current (not older than 10 years) throughout the contract performance period. The Contractor's Security Representative shall contact the Command Security Manager for guidance when reinvestigations are required.

Regardless of their duties or IT access requirements ALL contractor employees shall in-process with the Navy Command's Security Manager upon arrival to the Navy command and shall out-process prior to their departure at

the completion of the individual's performance under the contract. Employees requiring IT access shall also check-in and check-out with the Navy Command's Information Assurance Manager. Completion and approval of a System Authorization Access Request Navy (SAAR-N) form is required for all individuals accessing Navy Information Technology resources. The SAAR-N shall be forwarded
to the Navy Command's Security Manager at least 30 days prior to the individual's start date. Failure to provide the required documentation at least 30 days prior to the individual's start date shall result in delaying the individual's start date.

The contractor shall ensure that each contract employee requiring access to IT systems or networks complete annual Information Assurance (IA) training, and maintain a current requisite background investigation. Contractor employees shall accurately complete the required investigative forms prior to submission to the Navy Command Security Manager. The Navy Command's Security Manager will review the submitted documentation for completeness prior to submitting it to the Office of Personnel Management (OPM). Suitability/security issues identified by the Navy may render the contractor employee ineligible for the assignment. An unfavorable determination made by the Navy is final (subject to SF-86 appeal procedures) and such a determination does not relieve the contractor from meeting any contractual obligation under the contract. The Navy Command's Security Manager will forward the required forms to OPM for processing. Once the investigation is complete, the results will be forwarded by OPM to the DON Central Adjudication Facility (CAF) for a determination.

If the contractor employee already possesses a current favorably adjudicated investigation, the contractor shall submit a Visit Authorization Request (VAR) via the Joint Personnel Adjudication System (JPAS) or a hard copy VAR directly from the contractor's Security Representative. Although the contractor will take JPAS "Owning" role over the contractor employee, the Navy Command will take JPAS "Servicing" role over the contractor employee during the hiring process and for the duration of assignment under that contract. The contractor shall include the IT Position Category per SECNAV M-5510.30 for each employee designated on a VAR. The VAR requires annual renewal for the duration of the employee's performance under the contract.

BACKGROUND INVESTIGATION REQUIREMENTS AND SECURITY APPROVAL PROCESS FOR CONTRACTORS ASSIGNED TO OR PERFORMING NON-SENSITIVE DUTIES

Contractor employee whose work is unclassified and non-sensitive (e.g., performing certain duties such as lawn maintenance, vendor services, etc ...) and who require physical access to publicly accessible areas to perform those duties shall meet the following minimum requirements:

- Must be either a US citizen or a US permanent resident with a minimum of 3 years legal residency in the United States (as required by The Deputy Secretary of Defense DTM 08-006 or its subsequent DoD instruction) and
- Must have a favorably completed National Agency Check with Written Inquiries (NACI) including a FBI fingerprint check prior to installation access.

To be considered for a favorable trustworthiness determination, the Contractor's Security Representative must submit for all employees each of the following:

- SF-85 Questionnaire for Non-Sensitive Positions
- Two FD-258 Applicant Fingerprint Cards (or an electronic fingerprint submission)
- Original Signed Release Statements

The contractor shall ensure each individual employee has a current favorably completed National Agency Check with Written Inquiries (NACI) or ensure successful FBI fingerprint results have been gained and investigation has been processed with OPM.

Failure to provide the required documentation at least 30 days prior to the individual's start date may result in delaying the individual's start date.

* Consult with your Command Security Manager and Information Assurance Manager for local policy when IT-III (non-sensitive) access is required for non-US citizens outside the United States.

(end text)

Enterprise Contractor Manpower Reporting Application (ECMRA)
The contractor shall report contractor labor hours (including subcontractor labor hours) required for performance of services provided under this contract via a secure data collection site. Contracted services excluded from reporting are based on Product Service Codes (PSCs). The excluded PSCs are:
(1) W, Lease/Rental of Equipment;
(2) X, Lease/Rental of Facilities;
(3) Y, Construction of Structures and Facilities;
(4) S, Utilities ONLY;
(5) V, Freight and Shipping ONLY.

The contractor is required to completely fill in all required data fields using the following web address https://doncmra.nmci.navy.mil.

Reporting inputs will be for the labor executed during the period of performance during each Government fiscal year (FY), which runs October 1 through September 30. While inputs may be reported any time during the FY, all data shall be reported no later than October 31 of each calendar year. Contractors may direct questions to the help desk, linked at https://doncmra.nmci.navy.mil.

Pursuant to FAR 52.232-18, funds are not presently available for this contract. The Government's obligation under this contract is contingent upon the availability of appropriated funds from which payment for contract purposes can be made. No legal liability on the part of the Government for any payment may arise until funds are made available to the Contracting Officer for this contract.

The notice of availability of funds issued pursuant to this clause will be posted to the NAVSUP Fleet Logistics Center (FLC) Norfolk web page at:
http://www.navsup.navy.mil/navsup/ourteam/navsupgls/prod_serv/contracting/con_navsupflcn.

(end text)

The information provided in this section is strictly a summary of the applicable SOFAs and country-specific requirements and should not be construed as all-inclusive. It is the contractor's responsibility to review, understand and comply with all SOFA and country-specific requirements applicable to this contract.

SOFA status defines the benefits received by the contractor and/or the contractor’s dependents. These benefits include, but are not limited to, commissary, postal, military banking privileges, on-base education and access to United States military medical facilities. The SOFA status usually defines the prosecution for criminal offenses in the USG OCONUS court system and laws as opposed to the Host Nation judicial system and laws but that will vary by location.

The Government may, at the discretion of the Base Commander, provide contractor employees and authorized dependents logistics support as mentioned in the previous paragraph. This only applies to foreign countries that have a SOFA.

The NATO SOFA is the governing document with respect to the status of forces in NATO countries. The NATO SOFA is silent to many issues, such as how and when SOFA status is granted to contractors. Issues like this are addressed in various bilateral agreements that the United States has with other countries, and the requisite requirements differ from country to country.

1.1.1. BASE PRIVILEGES - BAHRAIN AND CONTRACTOR LICENSING IAW BAHRAIN LAW:

Contractor shall be aware of the requirements for foreign companies wishing to do business in Bahrain must be registered and licensed carry out any commercial activity IAW with Bahrain Commercial Companies Law No. (21) of 2001. All contractor employees shall possess a valid working visa. The Government will not sponsor contractors. Working visas shall be the responsibility of the employee or sponsored by the Contractor.

Without additional expense to the Government, the contractor shall be responsible for obtaining any necessary insurance, licenses, and permits and for complying with any applicable laws, codes, and regulations required by the host-nation in connection with the performance of the work set forth in this contract. The Government will not be responsible for activities of the contractor or contractor employees outside the scope of this contract. The Government has no obligation to support the dependents of contractor employees, including, but not limited to, providing command sponsorship within the host-nation.

1.1.1.1. DOD CONTRACTOR Insurance (Bahrain)

No mandatory requirements for insurance exist

1.1.2. DOD CONTRACTOR PERSONNEL OFFICE (DOCPER) COMPLIANCE (NAPLES)

The contractor shall comply with the procedures associated with the Department of Defense Office of Civilian Personnel guidelines for employing DoD contractor employees as Technical Representatives (TRs) in Italy. The Web site for obtaining the documentation that governs the Technical Representative Accreditation Procedures in Italy, of DoD contractor employees as TRs, is identified below. The Government will also use the Contractor Verification System (CVS) to validate the contractor's need and application information for a CAC. The Government will reimburse the contractor for all costs associated with the DOCPER process.

http://www.per.hqusareur.army.mil/CPD/DocPer/Italy/ItalyDefault.aspx

1.1.2.1. DOD CONTRACTOR Insurance (Italy)

No mandatory requirements for insurance exist

1.1.3. DOD CONTRACTOR SOFA Status (Japan)

Article XIV gives SOFA status to a company, not to the individual employees, as is the case under SOFA Article I(b). Under Article XIV, only the actual employees receive SOFA benefits. There are no benefits for the employees' dependents. Article XIV is limited to United States companies present in Japan solely to work for the United States Forces, Japan (USFJ). Article XIV requires a two to three year application process.

U.S. citizen contractors not ordinarily resident in Japan and present in Japan at the official invitation of the USG for the performance of a contract for the United States armed forces may be given SOFA Article I(b) status. The number of employees does not affect whether Article I(b) or Article XIV status is appropriate.

1.1.3.1. DOD CONTRACTOR Insurance (Japan)

Determining and meeting these requirements are the responsibility of the contractor, at no additional expense to the Government.

(end of text)